UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,673	01/22/2004	Frederic Perriot	20423-08166	7489

34415 7590 06/03/2009

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
06/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	Application No.	Applicant(s)	
	10/763,673	PERRIOT, FREDERIC	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,4,6-19 and 24-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,4,6-19 and 24-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 3, 4, 6-19 and 24-28 are pending.

This Office Action is in response to amendment filed 11/05/2008

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 3, 4, 6-19, 24-26, and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Christodorescu (US 2005/0028002)** in view of **Nachenberg (US 5,826,013),** hereafter "Nachenberg".

Considering **Claims 6 and 24,** Christodorescu discloses a computer-implemented method for determining whether computer code contains malicious code (abstract), said method comprising the steps of: identifying computer code suspected of currently containing malicious code ([0011]), the computer code having a decryption loop and a body ([0006], [0009]), and responsive to the malicious code detection procedure detecting malicious code in the optimized loop code or the malicious code detection protocol detecting malicious code in the optimized body code ([0011]-[0028]), declaring a confirmation that the computer code contains malicious code ([0011], [0031]).

Christodorescu does not explicitly disclose optimizing the decryption loop to produce optimized loop code; performing a malicious code detection procedure on the optimized loop code; optimizing the body to produce optimized body code; subjecting the optimized body code to a malicious code detection protocol; Christodorescu suggests that both the loop and body of the suspected computer code are optimized ([0009], [0011]).

The combination of Christodorescu and Nachenberg discloses optimizing the decryption loop to produce optimized loop code (Nachenberg- column 1- lines 63-67, column 2- lines 1-25, Christodorescu- [0011]); performing a malicious code detection procedure on the optimized loop code (Christodorescu- [0011]); optimizing the body to produce optimized body code (Nachenberg- column 1- lines 63-67, column 2- lines 1-25, Christodorescu- [0011]); subjecting the optimized body code to a malicious code detection protocol (Christodorescu- [0011]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Christodorescu by treating the loop code and body code separately as taught by Nachenberg in order to provide polymorphic virus detection systems that can be readily expanded to cover newly discovered viruses, without need for extensive regression testing and modification of the heuristics of the emulation control module. In addition, the system should be able to provide accurate results without emulating unnecessarily large numbers of instructions (Nachenberg- column 2- lines 44-50).

Considering **Claims 3 and 26,** the combination discloses the optimizing step comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction (Christodorescu [0011]-[0028]).

Considering **Claim 4,** Christodorescu discloses at least two of said techniques are combined synergistically (Christodorescu- [0011]-[0028])

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Christodorescu by treating the loop code and body code separately as taught by Nachenberg in order to provide polymorphic virus detection systems that can be readily expanded to cover newly discovered viruses, without need for extensive regression testing and modification of the heuristics of the emulation control module. In addition, the system should be able to

provide accurate results without emulating unnecessarily large numbers of instructions (Nachenberg- column 2- lines 44-50).

Considering **Claims 7 and 28,** the combination discloses the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning (Christodorescu- [0027], [0066], Nachenberg- abstract).

Considering **Claim 8,** the combination discloses the optimizing step comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction (Christodorescu- [0011]-[0028]).

Considering **Claim 9,** the combination discloses the step of optimizing the body comprises using at least one output from the group of steps consisting of optimizing the decryption loop and performing a malicious code detection procedure on the optimized loop code (Christodorescu- [0011], Nachenberg- column 3- lines 35-53).

Considering **Claim 10,** the combination discloses the step of performing a malicious code detection procedure on the optimized loop code indicates the presence of malicious code in the computer code, the steps of optimizing the body and subjecting the optimized body code to a malicious code detection protocol are aborted (Christodorescu-[0031]).

Considering **Claim 11,** the combination discloses the additional step of, after the step of performing a malicious code detection procedure on the optimized loop code, revealing an encrypted body (Nachenberg- column 6- lines 10-31).

Considering **Claim 12,** the combination discloses the step of revealing an encrypted body comprises emulating the optimized loop code (Nachenberg- column 6- lines 10-31).

Considering **Claim 13,** the combination discloses the step of revealing an encrypted body comprises applying a key gleaned from the optimized loop code (Nachenberg- column 5- lines 52-61, column 6- lines 10-31).

Considering **Claim 14,** the combination discloses optimizing the computer code to produce optimized code comprises: performing a forward pass operation (Christodorescu- [0017], [0019], [0020], [0023]; performing a backward pass operation (Christodorescu- [0018], [0021]); performing a control flow graph reduction (Christodorescu- [0044]-[0045]); and iterating the above three steps a plurality of times (Christodorescu- [0044]-[0046]).

Considering **Claim 15,** the combination discloses the iteration of the three steps stops after either: a pre-selected number of iterations; or observing that no optimizations of the computer code were performed in the most recent iteration (Christodorescu- [0060]-[0065], Fig. 2).

Considering **Claim 16,** the combination discloses the step of performing a code motion procedure, wherein the four steps are iterated a plurality of times (Christodorescu- [0018],[0024]).

Considering **Claim 17,** the combination discloses the forward pass operation comprises one or more steps from the set consisting of: peephole optimization; constant folding; copy propagation; forward computations related to abstract interpretation; and instruction specialization (Christodorescu- [0011]-[0028]).

Considering **Claim 18,** the combination discloses the backward pass operation comprises one or more steps from the set consisting of backward computations related to abstract interpretation and local dead code elimination (Christodorescu- [0018], [0021]).

Considering **Claim 19,** the combination discloses the backward pass operation comprises the additional step of global dead code elimination (Christodorescu- [0021]).

Considering **Claim 25**, the combination discloses the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning (Christodoresco- [0027]).

2. **Claim 27** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Christodorescu** and **Nachenberg** in view of **Teblyashkin et al. (US 7,266,844)**, hereafter "Teblyashkin".

Considering **Claim 27,** the combination of Christodorescu and Nachenberg does not explicitly disclose determining whether computer code contains malicious code, said method comprising the steps of: performing a dead code elimination procedure on the computer code; noting the amount of dead code eliminated during the dead code elimination procedure; and when the amount of dead code eliminated during the dead

code elimination procedure exceeds a preselected dead code threshold, declaring a suspicion of malicious code in the computer code.

Teblyashkin discloses determining whether computer code contains malicious code (abstract), said method comprising the steps of: performing a dead code elimination procedure on the computer code (column 1- lines 31-38); noting the amount of dead code eliminated during the dead code elimination procedure (column 1- lines 39-42); and when the amount of dead code eliminated during the dead code elimination procedure exceeds a preselected dead code threshold (column 1- lines 43-62), declaring a suspicion of malicious code in the computer code (column 1- lines 39-42).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by determining whether computer code contains malicious code, said method comprising the steps of: performing a dead code elimination procedure on the computer code; noting the amount of dead code eliminated during the dead code elimination procedure; and when the amount of dead code eliminated during the dead code elimination procedure exceeds a preselected dead code threshold, declaring a suspicion of malicious code in the computer code as taught by Teblyashkin in order to detect polymorphic viruses which are otherwise difficult to detect (Teblyashkin- column 1- lines 60-62).

Response to Arguments

The Final Office action dated 2/20/2009 incorrectly rejected Claim 27 under 35 USC 102. Claim 27 is dependent on Claim 6 which was rejected under 35 USC 103(a).

Claim 27 is now rejected under 35 USC 103(a) as being unpatentable over Christodorescu and Nachenberg in view of Teblyashkin.

Applicant's arguments filed 4/14/2009 with respect to Claims 6, 9-14, and 28 have been fully considered but they are not persuasive.

Regarding **Claims 6, and 9-14,** applicants' arguments have been fully considered but are not persuasive. With respect to applicants argument that the combination fails to teach *optimizing the decryption loop to produce optimized loop code; performing a malicious code detection procedure on the optimized loop code,* applicant is directed to Nachenberg- column 1- lines 63-67, column 2- lines 1-25, Christodorescu- [0011] Nachenberg- column 6- lines 54-67 and column 7- lines 1-8. Nachenberg discloses "a static exclusion module 230 and a dynamic exclusion module 240, which combine to substantially reduce the number of file instructions" (i.e. optimize the code). The substantial reduction in the number of file instructions as taught by Nachenberg could reasonably be interpretted to be "code optimization" as recited in the claim.

Regarding **Claim 28,** applicant's arguments have been fully considered but are not persuasive. With respect to applicant's argument that the combination fails to teach emulation, applicant is directed to Christodorescu- [0027], [0066], Nachenberg- abstract. Malicious code detection via emulation is a well known technique within the art as shown by the cited references.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435
4/27/2009
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2435